REMARKS

Claims 1-5, 7-13, 15-20 and 22-26 were pending and stand rejected. Claims 1, 9, 16, and 23 have been amended.

Rejection under 35 USC 101

Claims 1-5, 7-8, 16-20 and 22-24 were rejected under 35 USC 101 as allegedly being directed to non-statutory subject matter. Claim 1 previously recited "a first distributed software agent to…", "a second distributed software agent to…", and "a manager module … to …." Claim 1 has been amended to recite "a first distributed software agent comprising a processor configured to…", "a second distributed software agent comprising a processor configured to…", and "a manager module …, the manager module comprising a processor configured to …" and complies with 35 USC 101. Claims 2-5 and 7-8 depend from claim 1 and also comply with 35 USC 101.

Claim 23 previously recited "a plurality of distributed software agents to…" and "a manager module … to …." Claim 23 has been amended to recite "a plurality of distributed software agents, each comprising a processor configured to…" and "a manager module …, the manager module comprising a processor configured to …" and complies with 35 USC 101. Claim 24 depends from claim 23 and also complies with 35 USC 101.

Regarding claim 16, Applicant traverses the Examiner's rejection. Claim 16 recites a machine readable medium, which is an article of manufacture. An article of manufacture is statutory subject matter. Therefore, claim 16 complies with 35 USC 101. Claims 17-20 and 22 depend from claim 16 and also comply with 35 USC 101.

Rejection under 35 USC 103(a)

Claims 1-3, 5, 7-11, 13, 15-18, 20, and 22-26 were rejected under 35 USC 103(a) as allegedly being unpatentable over Porras (US 6,704,874 B1) in view of Pifer (US 4,914,444) and Halstead (US 5,896,524). Applicant respectfully traverses in view of the amended claims. For the record, Applicant also traverses the Examiner's assertions regarding the motivation to combine Porras, Pifer, and Halstead. As amended, claim 1 recites in part:

> determine, based on the first alert and the second alert, whether the first clock and the second clock are synchronized; and
> if the first clock and the second clock are not synchronized:
> synchronize the first clock and the second clock;
> modify at least one of a timestamp within the first alert and a timestamp within the second alert; and
> correlate the first alert and the second alert according to a rule, which comprises determining whether the first alert and the second alert satisfy a condition of the rule.

As described in the pending application, the claimed invention comprises a first software agent, a second software agent, and a manager module (¶¶12-15; FIG. 1). The manager module receives a first stream of alerts from a first network security device having a first clock and a second stream of alerts from a second network security device having a second clock (¶22). The manager module identifies a first alert in the first stream and a second alert in the second stream, wherein the first alert includes an Internet Protocol (IP) address, and wherein the second alert includes the IP address (¶¶23-24). The manager module determines, based on the first alert and the second alert, whether the first clock and the second clock are synchronized (¶26). If the first clock and the second clock are not synchronized, the manager module synchronizes the first clock and the second clock (¶26), modifies at least one of a timestamp within the first alert and a timestamp within the second alert (¶36), and correlates the first alert and the second alert according to a rule (¶17).

In one embodiment, a manager module uses a rules engine to correlate alerts based on correlation rules and to produce meta-alerts (higher level alerts) (¶¶14-15, 17; FIG. 1). For example, one rule may be that if twenty or more unsuccessful logins are followed by a successful login from the same IP address, then a high-level alert representing a successful brute force dictionary attack is generated (¶17). Correlating the first alert and the second alert according to a rule comprises determining whether the first alert and the second alert satisfy a condition of the rule (¶17).

A rule can be time-sensitive (¶18). For example, the rule above can be modified to require that the twenty or more unsuccessful logins occur within a one minute time period (¶18). If the login events include incorrect timestamps due to the clocks not being synchronized, the rule will not work as intended (¶21). Thus, in order to solve this problem, if the first clock and the second clock are not synchronized, at least one of a timestamp within the first alert and a timestamp within the second alert will be modified before the first alert and the second alert are correlated according to the rule (¶21).

Applicant agrees with the Examiner that Porras does not disclose, teach, or suggest "if the first clock and the second clock are not synchronized: … correlate the first alert and the second alert according to a rule" (Detailed Action, p. 4). It follows that Porras also does not disclose, teach, or suggest the claimed element "if the first clock and the second clock are not synchronized: … correlate the first alert and the second alert according to a rule, which comprises determining whether the first alert and the second alert satisfy a condition of the rule."

Pifer does not remedy this deficiency. Pifer discusses a synchronization system and method for a lightning location system having a plurality of remote lightning detectors transmitting data to a lightning position analyzer (Abstract). Each of the detectors includes a

clock for identifying the time of occurrence of a detected lightning discharge (3:34-36). The position analyzer identifies data from one detector and data from another detector that represent the same lightning discharge. The position analyzer then synchronizes the detectors utilizing the lightning discharge itself as an external time reference (3:52-56). The difference between the times of occurrence as measured by the first and second detectors for the lightning event is calculated and used to correct the time of occurrence data for each lightning event detected by the second detector (4:35-40). Assume, *arguendo*, that the correction to the time of occurrence data corresponds to the claimed element "modify at least one of a timestamp within the first alert and a timestamp within the second alert."

Pifer does not disclose, teach, or suggest the claimed element "if the first clock and the second clock are not synchronized: … correlate the first alert and the second alert according to a rule, which comprises determining whether the first alert and the second alert satisfy a condition of the rule." In Pifer, after the lightning time of occurrence data from each detector has been corrected, the corrected data is simply stored. Pifer does not disclose, teach, or suggest determining whether the corrected data satisfies a condition of a rule, as recited in claim 1.

Halstead does not remedy this deficiency. Halstead discloses determining a global time base from the local clocks' data in a multiprocessor system (abstract). An intermediate time base is determined from a pair of selected processors (3:17-18). Clock drift and offset parameters are calculated for the local clocks (3:19-20). These values are used to modify the time stamps of events in a global event log (3:33-34). Assume, *arguendo*, that the modification of the time stamps of events in the global event log corresponds to the claimed element "modify at least one of a timestamp within the first alert and a timestamp within the second alert."

Halstead does not disclose, teach, or suggest the claimed element "if the first clock and the second clock are not synchronized: … correlate the first alert and the second alert according to a rule, which comprises determining whether the first alert and the second alert satisfy a condition of the rule." In Halstead, after the time stamps of events in the global event log have been modified, the modified data is simply stored. Halstead does not disclose, teach, or suggest determining whether the modified data satisfies a condition of a rule, as recited in claim 1.

Thus, claim 1 (as amended) is patentable over Porras, Pifer, and Halstead, both individually and in combination. Independent claims 9, 16, and 23 (as amended) recite similar language and are also patentable over Porras, Pifer, and Halstead, both individually and in combination, for at least the same reasons.

Claims 4, 12, and 19 were rejected under 35 USC 103(a) as being unpatentable over Porras in view of Pifer, Halstead, and Apel. Applicant respectfully traverses. For the record, Applicant also traverses the Examiner's assertions regarding the disclosure of Apel and regarding the motivation to combine Porras, Pifer, Halstead, and Apel.

The claims not specifically mentioned above depend from claims 1, 9, 16, or 23 (directly or indirectly), which were shown to be patentable over Porras in view of Pifer and Halstead. In addition, these claims recite other features not included in claims 1, 9, 16, or 23. Thus, these claims are patentable over Porras in view of Pifer and Halstead, for at least the reasons discussed above, as well as for the elements that they individually recite.

Applicant respectfully submits that the pending claims are allowable over the cited art of record and requests that the Examiner allow this case. The Examiner is invited to contact the undersigned in order to advance the prosecution of this application.

Respectfully submitted,

HUGH S. NJEMANZE

Dated: August 18, 2008

By: /Sabra-Anne R. Truesdale/

Sabra-Anne R. Truesdale
Reg. No. 55,687
Fenwick & West LLP
Silicon Valley Center
801 California Street
Mountain View, CA 94041
Tel. (650) 335-7187
Fax (650) 938-5200